IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

In re patent application:

Appl. No.	:	10/797,547	Confirmation No.:4408
Applicant	:	Jay M. McNally, et al.	
Filed	:	March 10, 2004	
Art Unit	:	2113	
Examiner	:	Charles Ehne	
Attorney Docket No. :		G-231	Date: September 10, 2007

Mail Stop Appeal Brief- Patents
Commissioner for Patents
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Appellants respectfully submit the following Brief in the appeal of the subject application. This Brief is in furtherance of the Notice of Appeal filed in this case on July 11, 2007, following a Final Office Action mailed April 13, 2007, rejecting claims 1 -20.

The Commissioner is hereby authorized to charge any additional fees that may be required for this appeal or to make this brief timely or credit any overpayment to Deposit Account No. 16-1885.

TABLE OF CONTENTS

This Brief contains these items under the following headings and in the order set forth below:

I.   REAL PARTY IN INTEREST

The real party in interest is Ibis Consulting, Inc., the assignee of this application, and a wholly owned subsidiary of Pitney Bowes Inc., a Delaware corporation.

II.   RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences known to Appellants, their legal representative, or the assignee that will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III.   STATUS OF CLAIMS

(1) Claims 1-20 are the subject of this Appeal, and stand rejected under 35 U.S.C. §102(e) as allegedly anticipated by US-2004/020485 to Vargas et al. ("Vargas").

(2) Appellants hereby appeal the rejection of claims 1-20.

IV.   STATUS OF THE AMENDMENTS

(1) Claims 1-14 were filed with the application on March 10, 2004. In an Amendment dated January 5, 2007, claims 1 and 8 were amended, and claims 15-20 were added. A Corrected Amendment was filed on January 31, 2007. In response to a Final Office Action mailed April 13, 2007, Appellants filed an Amendment After Final Rejection on June 12, 2007 to address the Examiner's 35 U.S.C. §112, second paragraph rejection. In an Advisory Action mailed on June 25, 2007, the Examiner notified Appellants that the Amendment would be entered.

Therefore, current claims 1-20 are set forth in Appendix A to this Brief.

V.   SUMMARY OF CLAIMED SUBJECT MATTER

The presently claimed invention is directed to systems and methods for recovering stored electronic data to determine modifications and deletions of the stored electronic data and for automatically analyzing those modifications and deletions to provide categorization information. Recovering, analyzing and categorizing this data is important, especially during litigation disputes, to determine the occurrences of certain events, and to determine the behavior of users of electronic data. For example, information embedded in electronic mail data, for typically indicates the sender, the recipients, and the time sent, and other data regarding the electronic mail message, whether or not this data is evident to the user. Such embedded data that, rather than being the content of the message, describes the details of the message creation and transmission, is called "metadata". "Metadata" is commonly described as "data about data" or data that tracks the history of an electronic document. Similar data about the creation and modification of electronic data relating to office documents such as word processing files, spreadsheet files, database files and other application files exists.

The presently claimed invention analyzes differences in stored file information beyond simple bit level differences that may fall out of check-sum comparisons. The invention analyzes stored data in order to identify and establish categories such as, for example, missing files which are missing as a result of deletion or moved and modified files, and files that have the same path but are different according to a calculated parameter, for example an MD5 hash value and/or metadata.

This information is determined through analyzing two sets of server restores on the files so that comparisons of MD5 and metadata may be made. Comparisons are made to determine, for example, whether the same file name, size and short path name are present. Differences are then analyzed. Based on this analysis, it is possible to determine whether the file is modified in place, moved or deleted for example. This anaylsis further identifies partial difference in

the two data sets that result from elimination of files with the same MD5 hash value. This is accomplished by analyzing the frequency of equivalent MD5 hash values. When multiple files are identified, subsequent short path analysis is performed to determine which occurrence was eliminated. This information can be relevant to litigation when a particular user who is identified deleted a particular file of interest. The analysis allows for a deterministic categorization of differences in files on two server images.

An example of the types of categories that are compared and analyzed is found in Fig. 2, which is reproduced below:
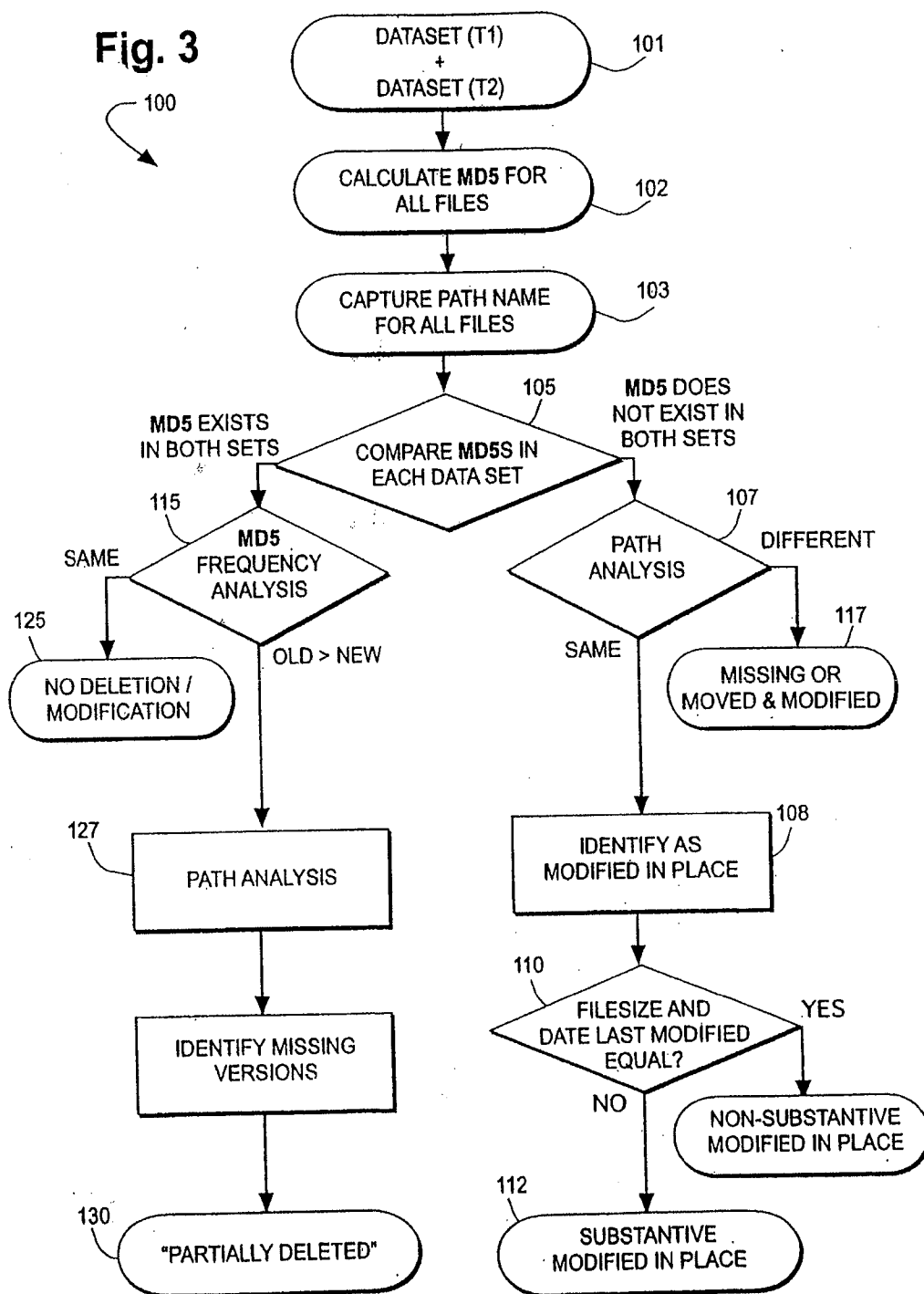
FIG. 2
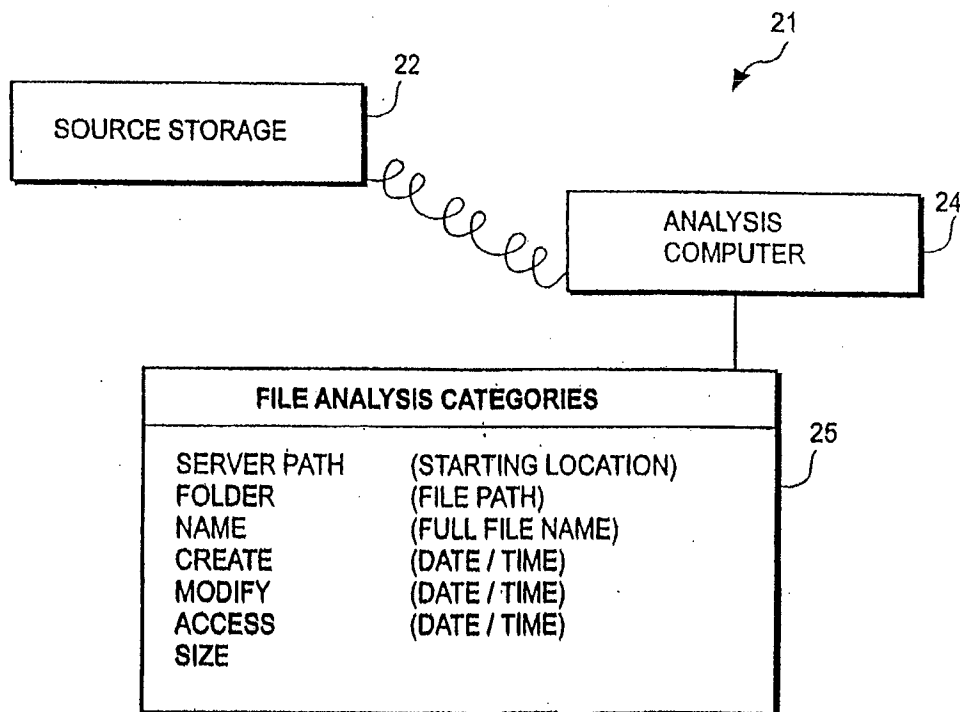
The analysis depicted in Fig. 2 can be used to compare two backup sessions from the same file server at different points in time, to determine if files were deleted or otherwise manipulated and how the data sets have changed. The inventive analysis of this preferred exemplary embodiment examines each source independently and collects information related to file content and characteristics of the file. Once the source is restored, metadata is gathered for each file within the data set. The exemplary list of fields of metadata captured for each file at element 25 of Fig. 2 includes:

Server path (starting location of the data)

Folder   (file path)

Name   (full file name)

Create   (date/time)

Modify   (date/time)

Access   (date/time)

Size

MD5 hash value

By doing this analysis, the presently claimed invention is able to identify "interesting differences", not simply bit level differences that would fall out of a check-sum comparison, for example the MD5 hash value for every file. By generating this information, files that have been "modified in place," that is, have the same path on each server but have different contents identified. A file is considered "modified" if, during the time period between the two snapshots being compared, a change was made to the file resulting in a change to the MD5 hash value. An example of another comparison that takes place is to see if a file is missing from the data set by comparing the file path, and file names between the two sets.

The presently claimed invention uses the data comparison analysis for the purpose of automatically generating file categorizations which designate categories of activities that have taken place with respect to files that have been altered from a first time period to a second time period. This process is generally shown in Fig. 3, which is reproduced below:

Fig. 3

100

DATASET (T1)
+
DATASET (T2) —— 101

↓

CALCULATE **MD5** FOR
ALL FILES —— 102

↓

CAPTURE PATH NAME
FOR ALL FILES —— 103

↓

105

MD5 EXISTS
IN BOTH SETS

COMPARE **MD5S** IN
EACH DATA SET

MD5 DOES
NOT EXIST IN
BOTH SETS

115

SAME

MD5
FREQUENCY
ANALYSIS

PATH
ANALYSIS

DIFFERENT

107

125

NO DELETION /
MODIFICATION

OLD > NEW

SAME

MISSING OR
MOVED & MODIFIED

117

127

PATH ANALYSIS

IDENTIFY AS
MODIFIED IN PLACE

108

↓

↓

110

IDENTIFY MISSING
VERSIONS

FILESIZE AND
DATE LAST MODIFIED
EQUAL?

YES

↓

NO

NON-SUBSTANTIVE
MODIFIED IN PLACE

130

"PARTIALLY DELETED"

112

SUBSTANTIVE
MODIFIED IN PLACE

As is seen from Fig. 3, the presently claimed system may be utilized to establish categories of at least:

1.   Missing files, either:

       (a)   Truly missing, as a result of, for example, deletion, or

       (b)   Moved and modified

2.   Modified files, those that have the same path, but different MD5 hash value and metadata.

This analysis allows for deterministic categorization of differences in files as either Missing, Modified v. Partially Deleted. Accordingly, this presently claimed invention can distinguish between these categories, and not merely identify that a change has been made to a file

Independent claim 1 is directed to a system for recovering electronic documents archived in a data storage mechanism comprising:
a computer connected with said data storage mechanism (Fig. 1, elements 12, 14; page 8, lines 1-14), where the computer retrieves a stored data file comprising electronic document data information (Fig. 1, elements 12, 14; page 8, line 1 - page 9, line 9) and further wherein the retrieved stored data file is analyzed based on file content and file characteristics (Fig. 2, elements 22, 24, 25; page 11, line 22 - page 18, line 22), and categorized into one or more of a plurality of distinct categories (Fig. 3; page 19, lines 1- page 20, line 13).

Independent claim 8 is directed to a method for recovering electronic documents archived in a data storage mechanism comprising the steps of:
providing a computer with access to said data storage mechanism (Fig. 1, elements 12, 14; page 8, lines 1-14);
retrieving a stored data file comprising electronic document data information from the data storage mechanism (Fig. 1, elements 12, 14; page 8, line 1 - page 9, line 9); and further analyzing the retrieved stored data file based on file content

and file characteristics (Fig. 2, elements 22, 24, 25; page 11, line 22 - page 18, line 22), and categorizing into one or more of a plurality of distinct categories (Fig. 3; page 19, lines 1- page 20, line 13).

Independent claim 17 is directed to a method for recovering electronic documents archived in a data storage mechanism comprising the steps of: providing a computer with access to said data storage mechanism (Fig. 1, elements 12, 14; page 8, lines 1-14);
retrieving a stored data file comprising electronic document data information from the data storage mechanism (Fig. 1, elements 12, 14; page 8, line 1 - page 9, line 9);
analyzing the retrieved stored data file based on file content and file characteristics (Fig. 2, elements 22, 24, 25; page 11, line 22 - page 18, line 22), categorizing into one or more of a plurality of distinct categories (Fig. 3; page 19, line 1- page 20, line 13); and
comparing said stored data file to detect deletions or modifications (Fig. 3; steps 105, 107, 115, 117, 125; page 19, line 11- page 20, line 13).

This summary is not intended to supplant the description of the claimed subject matter as provided in claims 1-20 as recited in Appendix A and understood in light of the entire specification.

VI.   GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

(B)   Whether or not claims 1-20 are patentable under 35 U.S.C. § 102(e) as anticipated by US -2004/020485 to Vargas, et al. ("Vargas").

VII.   ARGUMENT

As Appellants discuss in detail below, the final rejection of Claims 1-20 is devoid of any factual or legal premise that supports the position of unpatentability. It is respectfully submitted that the rejection does not even meet

the threshold burden of presenting a <u>prima facie</u> case of unpatentability. For this reason alone, Appellants are entitled to the grant of a patent. <u>In re Oetiker</u>, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992).

A. <u>Claims 1-20 Are Not Anticipated Under 35 U.S.C. § 102(e) by Vargas.</u>

Claim 1-20 are in the case and under final rejection of the Examiner and stand rejected under 35 U.S.C. § 102(e) as allegedly anticipated by Vargas.

Appellants respectfully disagree with the rejection and urge its reversal for at least the reasons stated below:

To establish anticipation of the claims under § 102(e), the Examiner is required to show that every element or step of the claim is found in a single reference. "To anticipate a claim, a reference must disclose every element of the challenged claim and enable one skilled in the art to make the anticipating subject matter." <u>PPG Indus., Inc. v. Guardian Indus. Corp.,</u> 75 F.3d 1558, 1566, 37 U.S.P.Q.2D (BNA) 1618, 1624 (Fed. Cir. 1996). The Examiner has not satisfied this burden.

Independent claim 1 recites:

> A system for recovering electronic documents archived in a data storage mechanism comprising:
> a computer connected with said data storage mechanism, where the computer retrieves a stored data file comprising electronic document data information and further wherein <u>the retrieved stored data file is analyzed based on file content and file characteristics, and categorized into one or more of a plurality of distinct categories</u>. (emphasis added)

The underlined portion of independent claim 1 identifies a major distinction between the presently claimed invention and Vargas. Similarly,

independent claim 8 recites "<u>analyzing the retrieved stored data file based on</u> <u>file content and file characteristics, and categorizing into one or more of a</u> <u>plurality of distinct categories</u>." And, independent claim 17 recites "<u>analyzing</u> <u>the retrieved stored data file based on file content and file characteristics; a</u> <u>plurality of distinct categories;</u>"

The Vargas reference relied upon by the Examiner does not teach these underlined elements of the claimed invention, and more specifically does not analyzing for the purpose of categorizing to distinguish between a plurality of categories as is understood by one of ordinary skill in the art reading the claim language in light of the specification. To the contrary, Vargas is directed data synchronization between a mobile device and a computing device over a wireless link without categorizing. Vargas' synchronization is merely intended to ensure that the wireless device and computing device have the same data and are aligned properly.

Vargas at paragraph 0007 describes synchronization as:

> [0007] However, allowing the user to access and change their information from any desired source means that the devices must be able to communicate with each other to indicate changes to the information. The process of two devices sharing changes in the application and/or PIM information is known as synchronization.

Vargas' synchronization is consistent with the way "Synchronize" is defined in Webster's New World College Dictionary, 4th Edition, as:

> 1. to cause to agree in time or rate of speed: regulate (clocks, a flash gun and camera shutter, etc.) so as to make synchronous; 2. to assign (events, etc.) to the same date or period: represent as or show to be coincident or simultaneous; 3. film to align (the picture and soundtrack).

The synchronization process as described by Vargas is used to align data to make two devices have the same information. This is extremely different from the analyzing and categorizing claimed by the present invention.

The Vargas synchronization operations are scheduled based on a predetermined subset of user actions, and involve a mapping between instances of objects stored in object stores. These objects are identified by handles. Paragraph 0064 of Vargas describes these handles and objects as follows:

> [0064] Synchronization manager **748** manipulates reference store **750** to maintain a mapping between instances of objects stored in object stores **32** and **34** on computing device **14** and instances of the same objects stored in object stores **20** and **22** on mobile device **12**. <u>Objects are identified by handles which are created by providers **752** and **754**. The handles are opaque to synchronization manager **748**, in that synchronization manager **748** need not be concerned with the actual composition of the handles</u> although the handles are manipulated and stored by synchronization manager **748**. (emphasis added)

Having handles in Vargas that are <u>opaque</u> (i.e. not transparent; hard to understand), so the synchronization manager need not be concerned with the actual composition of the handles, teaches away from what is claimed in the present invention. It is these handles in Vargas that are compared to determine if synchronization is necessary, not the underlying data or objects (that comprise a plurality of fields or properties related to PIM's), such as the presently claimed metadata.

In fact, Vargas sets forth in paragraphs 0067 - 0070 various possibilities on how to format the handles that are compared by the synchronization manager, and states that formatting handles via their path names is problematic. Those paragraphs state as follows:

[0067] The handles stored in reference store **750** may be formatted in accordance with the following criteria so that synchronization providers and **752** and **754** can perform the specified functions:

[0068] (a) <u>Each handle may contain data that uniquely identifies an object - such an object identifier, an ID number, a full pathname for a file system object, etc.</u> This data may be persistent (in that it does not change for a particular object) and should not be reused for subsequently created objects. This data can be compared to determine whether two handles actually correspond to the same object. As is discussed below, <u>this can be problematic</u> for file system information, because the object identifier is typically the pathname and can be changed simply by renaming the file.

[0069] (b) It may be possible to derive some object order based on the handle

[0070] The handle may have some sort of time stamp information, or version number. This information can be compared to determine whether an object has changed since the last handle was recorded in reference store **750**. (emphasis added)

Instead of comparing the metadata (which is considered problematic in Vargas) and as is claimed in the present invention, Vargas teaches comparing time stamp information, or version number. This does not teach the present invention

Once Vargas determines that these opaque handles are changed, the system in Vargas arranges to have the objects exchanged without reference to their content and without categorizing. This process is explained in Vargas at paragraph 0082, which states:

[0082] In order to exchange objects with mobile device **12**, synchronization manager **748** continually calls the method IReplObjHandler:GetPacket to have an appropriate provider **752** or **754** obtain a packet of information to be transmitted to mobile device **12**. To handle a packet received from mobile device **12**, synchronization manager **748** calls IReplObjHandler::SetPacket. This acts to provide a packet of information received from mobile device **12** to a synchronization provider **754** for storage on its associated object store. Similar interfaces are called by synchronization manager **740** on mobile device **12**.

This Vargas synchronization process does not teach Appellants' process of analyzing and categorizing.

In summary, Vargas does not teach the use of file content or file characteristics information to categorize files. To the contrary, the present invention analyzes file content and file characteristics to categorize and identify any modifications, deletions of stored electronic data to evidence user behavior regarding the electronic data. Such behavior will identify missing or deleted files, moved files or modified files. This is accomplished by examining each data source and collecting information related to file content and file characteristics. Meta data is then gathered for each file within the data set, such as:

- Server path (starting location of the data)
- Folder (file path)
- Name (full file name)
- Create (data/time)
- Modify (date/time)
- Access (date/time)
- Size
- MD5 hash value

This metadata is then used to determine whether substantive modifications or deletions were made to a file.

The processing of the presently claimed data comparison analysis is for the purpose of generating file categorizations which designate categories of activities that have taken place with a respect to files that have been altered from a first time period to a second time period. The categorizations can include: (a) classification as a non-substantive modification and a designation that the file has been modified in place, (b) classification as a substantive modification in the same file storage location, (c) classification as missing or moved and modified file, or (d) classification as no deletion or modification of the file has been made. This process enables significant volumes of data to be processed in order to quickly and automatically classify tremendous amounts of data. These classifications enable the determination of the behavior of users of

electronic data. Vargas' synchronization process does not anticipate the presently claimed invention because it fails to analyze, categorize and identify these changes.

The dependent claims are patentable for the same reasons expressed above with respect to the independent claims.

VIII.   CONCLUSION

For the reasons advanced above, Appellants respectfully submit that claims 1-20 are patentable. Reversals of the rejections by the Examiner are respectfully requested.

Respectfully submitted,

/Joseph C. Kirincich/
Joseph C. Kirincich
Reg. No. 38,734
Attorney for Applicant
Telephone (203) 924-3847

PITNEY BOWES INC.
Intellectual Property and Technology Law Department
35 Waterview Drive, P.O. Box 3000
Shelton, CT 06484-8000

CLAIMS APPENDIX A

1. A system for recovering electronic documents archived in a data storage mechanism comprising:

a computer connected with said data storage mechanism, where the computer retrieves a stored data file comprising electronic document data information and further wherein the retrieved stored data file is analyzed based on file content and file characteristics, and categorized into one or more of a plurality of distinct categories.

2. The system of claim 1, wherein the computer is connected via a network connection to the data storage mechanism.

3. The system of claim 1, wherein the computer is connected via a wireless network connection to the data storage mechanism.

4. The system of claim 1, wherein the data storage mechanism is a hard drive.

5. The system of claim 1, wherein the data storage mechanism is a tape drive.

6. The system of claim 1, wherein the data storage mechanism is a DVD.

7. The system of claim 1, wherein the data storage mechanism is a CD-ROM.

8. A method for recovering electronic documents archived in a data storage mechanism comprising the steps of:

providing a computer with access to said data storage mechanism;

retrieving a stored data file comprising electronic document data information from the data storage mechanism; and further analyzing the retrieved stored data file based on

file content and file characteristics, and categorizing into one or more of a plurality of distinct categories.

9. The method of claim 8, wherein the computer is connected via a network connection to the data storage mechanism.

10. The method of claim 8, wherein the computer is connected via a wireless network connection to the data storage mechanism.

11. The method of claim 8, wherein the data storage mechanism is a hard drive.

12. The method of claim 8, wherein the data storage mechanism is a tape drive.

13. The method of claim 8, wherein the data storage mechanism is a DVD.

14. The method of claim 8, wherein the data storage mechanism is a CD-ROM.

15. The system of claim 1 wherein the stored data file is analyzed using the file's last modified date, file size, file path or MD5 hash value.

16. The method of claim 8 wherein said step of analyzing comprises analyzing the file's last modified date, file size, file path or MD5 hash values.

17. A method for recovering electronic documents archived in a data storage mechanism comprising the steps of:
providing a computer with access to said data storage mechanism;
retrieving a stored data file comprising electronic document data information from the data storage mechanism;
analyzing the retrieved stored data file based on file content and file characteristics;
categorizing into one or more of a plurality of distinct categories; and

comparing said stored data file to detect deletions or modifications.

18.　　The method of claim 17 wherein said step of analyzing comprises analyzing the file's last modified date, file size, file path or MD5 hash value.

19.　　The system of claim 1 further comprising a comparison of said stored data file to detect deletions or modifications.

20.　　The method of claim 8 further comprising comparing said stored data file to detect deletions or modifications.

EVIDENCE APPENDIX B

None

RELATED PROCEEDINGS APPENDIX C

None